Bundesamt
für Sicherheit in der
Informationstechnik

# Assurance Continuity Maintenance Report

## BSI-DSZ-CC-0915-2016-MA-04

## BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 002.030

from

## NXP Semiconductors Germany GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0915-2016.

The certified product itself did not change. The change is related to

- Disconnection and discontinuation of development and production sites
- Additional warehouse,
- Physical move of all TOE related servers to NXP,
- Takeover of the device personalization flow from Broadcom to NXP.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0915-2016 dated 25 February 2016 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0915-2016.

Common Criteria
Recognition Arrangement
for components up to
EAL4

Bonn, 9 August 2017

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

# Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 002.030, NXP Semiconductors Germany GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified development and production environment of the TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 002.030 itself did not change.

The change is related to the development and production environment:

- Disconnection and discontinuation of development and production sites
  - Irvine, CA USA, 5300 California Avenue, Irvine CA 92617
  - Data Center Irvine, 17400 Von Karman, Ave, Irvine, CA 92614
  - Andover, MA USA, 200 Brickstone Square #401 ANDOVER MA 01810
  - BSPL Singapore, 29 Woodlands Industrial Park E1 North Tech, Singapore 757716
  - UTAC Singapore, 5 Serangoon North Avenue 5, Singapore 554916
  - AMKOR, Kaohsiung, Taiwan, Nantze Export Processing Zone, Kaohsiung, 811Taiwan, R.O.C.
- Additional warehouse NXP Kaohsiung 10 CHIN 5TH ROAD, N.E.P.Z., 81170 KAOHSIUNG
- Physical move of all TOE related servers from Zayo Data Center Irvine to NXP Caesar development laboratory
- Takeover of the device personalization flow from Broadcom to NXP

An ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The Common Criteria assurance requirements:

ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the following sites:

- ASE Kaohsiung - ASE Kaohsiung Nantze Export Processing Zone, Kaohsiung, Taiwan, R.O.C

  - Type of site: WLBGA, Bumping, Final Test, Backend, Initialization and Pre-Personalization
- NXP San Diego (formerly: BRCM San Diego) - NXP Semiconductors San Diego, 16340 West Bernardo Drive, San Diego, California 92127, USA (formerly: Broadcom Corporation)
  - Type of site: Development, Engineering Sample handling, Data Center
- TSMC Hsinchu/ Tainan - Taiwan Semiconductor Manufacturing Company Ltd., Fab-14 (Mask and Wafer fabrication), 1, Nan-Ke North Rd., Science Park Tainan, 741 Taiwan, R.O.C, Fab-7 (GDS file import server), 121, Park Ave., 3, Science Park, Hsinchu 300-77, Taiwan, R.O.C
  - Type of site: Mask Data Prep, Mask & Wafer Fabrication
- ATKH Kaohsiung (formerly: APK) - Assembly & Test Kaohsiung (ATKH), #10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170, Taiwan, R.O.C (formerly: Assembly Plant Kaohsiung (APK))
  - Type of site: Warehouse

# Conclusion

The change to the TOE is at the level of development/production sites. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [8].

The Security Target [7] has not been updated within the scope of this procedure and is still valid for the TOE.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0915-2016 dated dated 25 February 2016 is of relevance and has to be considered when using the product.

### Additional obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [9].

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months[1] and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

This report is an addendum to the Certification Report [3].

# References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, Version 2.1, June 2012

[2] IAR BCM_SPS02 Secure Processing System, Impact Analysis Report ALC Maintenance, NXP Semiconductors, Rev. 1.1, 6 February 2017 (confidential document)

[3] Certification Report BSI-DSZ-CC-0915-2016 for BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 1.0 from Broadcom Corporation, Bundesamt für Sicherheit in der Informationstechnik, 25 February 2016

[4] Assurance Continuity Maintenance Report BSI-DSZ-2016-MA-01 for the BCM_SPS02 Secure Processing System with Firmware version 002.010 or 002.020 from Broadcom Corporation, Bundesamt für Sicherheit in der Informationstechnik, 1 June 2016

[5] Assurance Continuity Maintenance Report BSI-DSZ-2016-MA-02 for the BCM_SPS02 Secure Processing System with Firmware version 002.010 or 002.020 from Broadcom Corporation, Bundesamt für Sicherheit in der Informationstechnik, 27 July 2016

[6] Assurance Continuity Maintenance Report BSI-DSZ-2016-MA-03 for the BCM_SPS02 Secure Processing System with Firmware version 002.030 from NXP Bundesamt für Sicherheit in der Informationstechnik, 2 December 2016

1 In this case the eighteen month time frame is related to the date of the initial version [9] of the Evaluation Technical Report for Composite Evaluation als the updates made afterwards are not related to updates of AVA evaluation tasks.

[7] a) Security Target for the BCM_SPS02, Broadcom Corporation, Version 3.5, 28 September 2016 (confidential document)

b) Security Target Lite for the BCM_SPS02, Broadcom Corporation, Version 1.2, 28 November 2016 (sanitized public document)

[8] Configuration list, Rev. 2.4, 30. July 2017, NXP Semiconductors (confidential document)

[9] Evaluation Technical Report for Composite Evaluation for BCM_SPS02, TÜV Informationstechnik GmbH, Version 4, 18 February 2016

[10] Evaluation Technical Report Summary for BCM_SPS02, TÜV Informationstechnik GmbH, Version 4, 1 August 2017